INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Information Technology Management (ITM) Strategic Plan Supporting National Defense (ITM Strategic Plan), Version 1.0

B. DATE Report Downloaded From the Internet: 6 Aug 98

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #:) **Department of Defense**
Office of the Secretary of Defense
Washington, DC

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __PM__ **Preparation Date**: 6 Aug 98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Department of Defense

Information Technology Management (ITM) Strategic Plan *Supporting National Defense*

(ITM Strategic Plan)
Version 1.0

March 1997

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Forwarding memorandum, Word version, and User feedback form also available.

Table of Contents

Foreword

We are all working to find better ways of bringing available information technologies into our operational and support missions. We have successes, such as the Global Command and Control System (GCCS), and we strive for more.

The Information Technology Management Reform Act of 1996 (ITMRA) mandates that we improve our day-to-day mission processes and properly use information technology to support those improvements. Technology must be fielded in an orderly, fast, and efficient way. We must use streamlined acquisition processes, commercial off-the-shelf products and services, and outsourcing, as appropriate, to take advantage of industry capabilities. The information technology investment portfolio concept, as put forth in ITMRA, emphasizes the need to do a better job of prioritizing information technology capital investments and being accountable for results -- from each person individually up to mission commanders and Congress. Keeping our workforce, military and civilian, trained in new technologies and improved processes is critical to achieving savings. The law recognizes all this is in vain if our information is not be protected.

It is our job to implement management processes that speed up development and acquisition programs, be mindful of costs, and provide the best support to DoD's mission that we possibly can.

We are institutionalizing processes reflecting the full spirit and intent of the law. Senior management -- including civilian, military and political appointees -- understands implementation will take time, but we must proceed without hesitation.

All of us -- the OSD staff, the Joint Staff, Military Services and Defense Agencies -- need to change the way we do our jobs and improve mission accomplishment, fully exploiting information technology.

This strategic plan introduces a roadmap for pursuing improvements well into the next century. However, the execution of this plan requires the commitment to work together toward our common goals. It is in this context that DoD Component Chief Information Officers will develop individual plans that

- include specific initiatives and actions that reflect a jointness of purpose,
- provide a sound foundation for improving processes, and
- ensure resources are in the right place to support our mission.

This strategic planning process will be a trailblazing effort, but together we can get there. Success will require continued cooperation, accountability, and refinements. Our best efforts depend upon a strong commitment to openness and trust. We have the opportunity to make a difference. I urge your continued support.

Executive Summary

Information has a central role in national defense. Joint Vision 2010 -- "*America's Military: Preparing for Tomorrow*", the joint warfighting strategic plan, recognizes information superiority as the foundation for joint warfighting doctrine and concepts as we move towards 2010. Similarly, DoD corporate level goals 4 and 5 reveal a prominent strategic role for information as follows:

"4. Maintain U.S. qualitative superiority in support of national defense in key warfighting capabilities (e.g., information warfare, logistics)

5. Employ modern management tools, total quality principles, and best business practices to reduce costs and eliminate unnecessary expenditures, while maintaining required military capability across all DoD mission areas."

To meet this vast responsibility, the Department must have a strategic plan that addresses the management and use of information technology capabilities. Thus this Information Technology Management (ITM) Strategic Plan provides overall direction and guidance for managing the Department's information resources. It establishes the DoD shared vision for ITM, top goals and objectives, measures of performance, and strategies to accomplish the goals. Specifically, it:

- Links ITM to joint warrior operational needs and mission support needs.
- Helps coordinate and integrate ITM activities across functional areas and organizations.
- Creates broad mechanisms to systematically manage DoD ITM resources and programs.
- Complies with the Information Technology Management Reform Act of 1996 (ITMRA).
- Serves as a model plan for ITM strategic plans at other levels and in other functions.

Strategic plans create a common expectation of an integrated IT environment where IT components work together for customers. By the same token, active participation and cooperation of the various functional areas and organizations will magnify the benefits that derive from IT. To this end, the ITM Strategic Plan focuses on two critical success factors: the joint and coordinated activity of the Components, and the customer.

The customer orientation is part of the Department's priority to realign the way it does its business. This is clearly reflected in the ITM mission and vision statements.

Mission: Provide the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently.

Vision: Information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operations.

To help realize the ITM mission and vision, Section IV of the ITM Strategic Plan describes the strategic direction. (Sections I, II, and III provide the purpose, scope, introduction and structure.) Four goals describe areas of major change. Each goal statement is followed by a description and conceptual diagram to outline the context for the goal together with "outcome performance" and "models of excellence" to address ITMRA performance and benchmarking requirements. Objectives and strategies characterize broad actions needed to pursue each goal. In general this plan will capitalize on DoD Component programs and projects to accomplish the strategies under the direction of an office of primary responsibility (OPR) and with resource reporting aligned with OSD level Planning, Programming, and Budgeting System (PPBS) criteria.

Four goals characterize fundamental DoD critical success factors for ITM to realize the vision.

Goal 1, *"Become a mission partner"*, grounds ITM in our national defense mission using joint mission planning and analysis processes as the basis for defining information service and performance requirements.

Goal 2, *"Provide services that satisfy customer information needs"*, builds on Goal 1 requirements by using the customer/supplier model to meet mission service requirements.

Goal 3, *"Reform IT management processes to increase efficiency and mission contribution"*, captures the essence of ITMRA emphasizing the management process improvements that are needed to more effectively deliver information and services to DoD mission customers.

Goal 4, "*Ensure DoD's vital information resources are secure and protected*", reflects the pervasive impact of information assurance on DoD.

Section V defines the update cycle for this strategic plan, establishes requirements for DoD Component-level ITM Strategic Plans, and describes how this plan interfaces with the DoD PPBS. Appendices provide detailed guidelines for preparing DoD Component plans, programs, and performance measures as well as critical, near-term actions to advance each strategy.

This strategic plan provides a roadmap to capitalize on these developments to realize more efficient and effective mission support. The execution of this plan requires leadership and commitment to work together toward our common goals. It is in this context that DoD Component CIOs need to develop individual plans that include specific initiatives and actions that reflect a jointness and commonality of purpose and provide a sound foundation for improving processes and ensuring that resources are in the right place to support our mission. The top-level ITM Strategic Plan does not address specific programs or budgets. It serves as a framework for the development of more detailed DoD Component plans that identify specific programs and initiatives, and relate them back to the overall DoD mission.

The plan conforms to Government Performance and Results Act (GPRA), Information Technology Management Reform Act (ITMRA), Paperwork Reduction Act (PRA), and Office of Management and Budget (OMB) mandates and guidelines. This body of laws and regulations has created the opportunity to move from budget and acquisition centric decision making to mission, architecture, service and performance decision making.

The DoD CIO is the agency executive responsible for ensuring that the ITMRA mandate is executed within the full spirit and intent of the law. The extensive experience and talent of DoD information technology support personnel, the emerging private information capabilities, and strong Congressional guidance provide a wealth of new opportunities for improvement. All of DoD, the OSD staff, the Joint Staff, Military Services and Defense Agencies need to change the way we do our jobs to improve mission accomplishment and fully exploit information technology.

Table of Contents

I. Purpose and Scope

Purpose

The Information Technology Management (ITM) Strategic Plan provides overall Department of Defense (DoD) guidance for managing its information resources. The Plan establishes the DoD shared vision for ITM, top goals and objectives, measures of performance, and strategies to accomplish the goals. The Plan:

- Links ITM to joint warrior operational needs and mission support needs.
- Provides the long-term direction for ITM planning.
- Helps coordinate and integrate ITM activities across functional areas and organizations.
- Creates capstone mechanisms to systematically manage DoD ITM resources and programs.
- Complies with provisions of the Clinger-Cohen Amendment to the National Defense Authorization Act of 1996 that contains the Information Technology Management Reform Act of 1996 (ITMRA).

Scope

The ITM Strategic Plan pertains to Information Management, Information Technology, Information Resources Management, Information Systems, and Information Services activities across the DoD. It applies to all organizations in the Department, including the Office of the Secretary of Defense, the Joint Staff, the unified Commands, and the DoD Components. In this plan the term "DoD Components" will

be used to represent Military Departments and Defense Agencies and activities as a group. The Plan will apply to interfaces between the Department and external organizations including other Government agencies, the private sector, non-profit organizations, allies, coalition partners, North Atlantic Treaty Organization (NATO), and other alliances. The scope includes all DoD information technology, including National Security Systems (NSS), as defined in the ITMRA. It applies to all DoD activities that provide or use information, and oversee, plan, resource, develop/acquire, and operate information capabilities for the warfighter and those who support the warfighter.

II. Introduction

DoD's strategic guidance highlights the central role of information in national defense. Joint Vision 2010, the capstone joint warfighting strategic plan, recognizes information superiority as the foundation for new joint doctrine and concepts as we move towards 2010.

> *"Improvements in information and systems integration will ... impact future operations by providing decision makers with accurate information in a timely manner and ... gain dominant battlefield awareness... We must have information superiority; the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same..."*

Two DoD Corporate Level Goals included in DoD's implementation of the Government Performance and Results Act (GPRA) also reveal a prominent strategic role for information as follows:

> *"4. Maintain U.S. qualitative superiority in support of national defense in key warfighting capabilities (e.g., information warfare, logistics)*
>
> *5. Employ modern management tools, total quality principles, and best business practices to reduce costs and eliminate unnecessary expenditures, while maintaining required military capability across all DoD mission areas."*

DoD has been and continues to be an information technology leader. We have been at the forefront of new technology, either as the creator, developer, or user. Our commanders, researchers, academia, and support contractors fervently pursue new technologies to maintain our military superiority. Congress and the American people recognize the importance of these initiatives and have provided the required resources to maintain that leadership. In return, many military innovations have found commercial equivalents with worldwide markets, especially information services.

Information technology is being used to improve mission effectiveness. Robust technical capabilities, information systems, methods and components influence every DoD activity. Information technology is integral to our intelligence, command and control, and support functions. Computers are a normal part of the work environment from office to warehouse. End to end operational threads, such as "sensor-to-shooter", are linked through information to achieve mission results in an ever more demanding environment, and create necessary efficiencies for the Department.

Information technology is a major component of most weapon systems with applications ranging from internal equipment control mechanisms to communicating plans and results. DoD business functions, such as logistics, finance, and personnel, employ information networks and process improvement to realize efficiencies in the face of continued downsizing. Managers routinely capture, save, and analyze information for planning, implementations, and tracking often using Commercial Off-the-Shelf (COTS) products. Architectures are developed to describe mission requirements and concepts, and software implements those concepts. The Defense Information Infrastructure (DII) has been defined to include all information resources. The DII Master Plan captures the essential elements of the DII and related roles and responsibilities.

Strategic plans create a common expectation of an integrated Information Technology (IT) environment where IT components work together for customers. To a degree we are victims of our own success.

Thousands of information systems have been optimized for a mission or organization. Now we have islands of IT capability, each trying to integrate with neighbors. Local optimization of these individual islands has made integration more difficult and intricate.

Industry and government are facing the same challenges of increasing global integration and demands for efficiency and downsizing. The nation as a whole, government and industry, has mobilized to find methods for increasing mission performance and organizational effectiveness such as total quality management, Baldrige Award for excellence, and business process improvement. The Government Performance and Results Act (GPRA) of 1993 and the ITMRA prescribe those techniques, together with information technology, to make government "work better and cost less". Extensive guidance from DoD, General Accounting Office (GAO), and other government and industry is now available as well as libraries of Baldrige Award winners and benchmarks for others to use as examples.

Technology transfer of military information capabilities to industry has been successful. Massive information industry investments are expected to continue resulting in more powerful and less costly products, services, and operational support capabilities. Simultaneously, Defense unique requirements for information and technology are expected to become more complex and require management attention and experienced personnel. Thus DoD must find ways of outsourcing work that can be performed by industry and concentrate in-house resources on core DoD mission areas. This provides the opportunity for the DoD IT community to commit a greater percentage of increasingly scarce management and technical resources to direct mission roles.

To realize the full benefits of the knowledge revolution, the information technology community must redesign and improve how it does its business. This will require significant changes in culture, organization, training, and processes. For example, the information technology professional must become a full partner with the warfighter in defining operational needs for information, and exploring promising new technologies. This Plan begins a process of reengineering how the Department delivers knowledge to warfighters and those who support them. Readers should focus on the strategic direction and new thrusts embodied in the Plan, and determine how they and the organizations they serve fit in this common framework, and how they can contribute to its success.

The Plan does not address specific programs or budgets. Implementation activities must first be guided by a common vision and strategic direction. The Department cannot achieve Joint Vision 2010, or its top goals, if it does not have a common strategy. The Plan does include near-term priority actions to move expeditiously forward on the implementation process. Each Component will develop its portfolio of information technology investments, based on identified criteria, to accomplish DoD goals and strategies.

ITMRA has created the opportunity to move from budget and acquisition centric decision making to mission, architecture, service and performance decision making. The Joint Vision 2010 and DoD Strategic plans have established the importance of information to the Department. The extensive experience and talent of DoD information technology support personnel, the emerging private information capabilities, and strong Congressional guidance provide a wealth of new opportunities for improvement. This strategic plan provides a roadmap to capitalize on these developments to realize more efficient and effective mission support. The nation expects and deserves our best efforts.

III. Strategic Plan Structure

The top-level ITM Strategic Plan serves as a framework for the development of more detailed DoD Component plans that identify specific programs and initiatives, and relate them back to the overall DoD mission. It outlines the priority information and information technology initiatives and facilitates the identification of common efforts and overlapping missions. These will be reviewed during planning and budget processes initially at the DoD Component level and also at OSD. The plan conforms to Government Performance and Results Act (GPRA), Information Technology Management Reform Act

(ITMRA), Paperwork Reduction Act (PRA), and Office of Management and Budget (OMB) and other mandates and guidelines.

Sections I, II, and III provide the purpose, scope, introduction and structure.

Section IV describes the strategic direction and contains the mission and vision which provide a common direction already part of some DoD strategic plans. Goals describe areas of major change to realize the vision.

Each goal statement is expanded in the same way. A description and conceptual diagram outline the context for the goal. A specific "outcome" paragraph describes successful realization of the goal with "outcome performance indicators" suggesting a set of quantitative representations. The "primary performance evaluation offices" ensure that performance information is collected and visible. "Models of excellence" recognized by Business Process Reengineering (BPR), Total Quality Management (TQM), or other communities provide examples of organizations or environments that have substantively achieved the goal. The examples illustrate the feasibility of the goal and provide concrete sources for case studies, partnering, and emulation.

Objectives and strategies characterize broad actions to pursue each goal. In general, DoD Component programs and projects will support and accomplish the strategies. The description for each strategy also identifies an office of primary responsibility (OPR) to track progress and a suggested OSD level Planning, Programming, and Budgeting System (PPBS) reporting area. Appendix B provides extracts from the Information Technology/Defense Information Infrastructure (DII) PPBS Reporting Structure describing the three major IT/DII areas: *Functional Automated Information System (AIS), Communications & Computing Infrastructure (C&CI), and Related Technical Activities (RTA).* DoD Component plans and programs implementing provisions of this strategic plan will use these areas to ensure OSD visibility.

Section V defines the update cycle for this strategic plan, establishes requirements for DoD Component-level ITM Strategic Plans, and describes how this plan interfaces with the DoD PPBS. Appendices A and B provide detailed guidelines for preparing DoD Component plans and programs. Appendix C identifies major sources of strategic information that need to be considered during each update cycle. Appendix D provides a list of specific performance indicators and targets that will be used to measure progress in achieving objectives and strategies. Appendix E specifically addresses critical, near-term actions to advance each strategy. Appendices D and E will be updated annually.

IV. DoD ITM Strategic Direction for the 21st Century

The mission and vision for information technology management (ITM) have a strong linkage to "supporting national defense". The mission statement is derived from the Command & Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance (C4ISR) Integration Task Force Report of November 1996.

Mission

Provide the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently.

The vision statement aligns ITM with Joint Vision 2010 and its emphasis on information dominance.

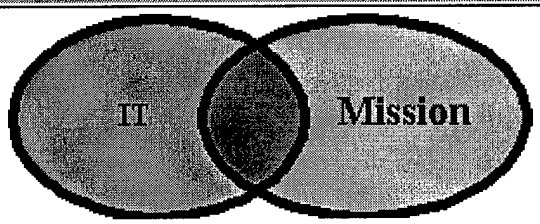
Vision

Information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operations.

Four goals characterize fundamental DoD critical success factors for ITM to realize the vision. Goal 1 grounds ITM in our national defense mission using joint mission planning and analysis processes as the basis for defining information service and performance requirements. Goal 2 builds on Goal 1 requirements by using the customer/supplier model to meet mission service requirements. Goal 3 emphasizes the management process improvements that are needed to more effectively deliver information and services to DoD mission customers. Goal 4 reflects the pervasive impact of information assurance on DoD. The strategies associated with the goals are organized logically but are intended to be implemented in parallel to make rapid progress toward the goals.

GOAL 1

Become a Mission Partner



Description: Achieving information dominance described in Joint Vision 2010 depends on comprehensive information and information technology (IT) support. IT is both an integral part of the mission environment and a support service function. Mission processes, information uses and services must be clearly understood and communicated to drive IT planning and resource decisions. The Department must leverage IT to improve the performance of mission processes and increase Departmental efficiency. IT must be applied to link end-to-end operational and support "threads" such as Sensor-to-Shooter. DoD can use ITMRA's "focus IT on mission" direction to address technical and managerial inhibitors to realize the full benefits of IT.

Outcome: IT organizations and personnel at all levels understand DoD's mission and the current and potential impacts of their products and services on that mission. Mission commanders and support managers have confidence in the IT communities' ability to support their IT requirements. Mission performance factors are accepted and routinely used in management decisions including resourcing and acquisition.

Outcome Performance Indicators:

1. Quality and coverage of mission area assessments linking IT to the mission,
2. Results of operational exercises (e.g. Joint Warfare Interoperability Demonstrations) and analyses at the DoD Decision Support Center (DSC) that demonstrate information capabilities and concepts, and
3. User surveys at all levels, including warfighter. Customer/user surveys include but are not limited to IT service support satisfaction and perceived response times.

Primary Performance Evaluation Office(s): Commander in Chiefs (CINCs), Joint Staff, Principal Staff Assistants (PSAs), and DoD Component Chief Information Officers.

Models of Excellence *(Organizations with seamless integration of IT and primary mission)*:

DoD Business Process Reengineering (BPR): Medical (OSD (Health Affairs)), Civilian Personnel, Commander in Chief, Strategic Command (CINCSTRATCOM), Deputy Undersecretary of Defense (Logistics), U. S. Marine Corps
DoD Presidential Quality Award Winners: Army Research, Development & Engineering Center, Defense Contract Management Command
Industry National Baldrige Award Winners: duPont Corp., IBM Corp., Motorola

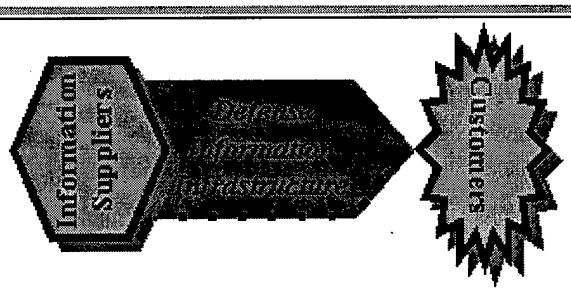
Objective 1.1 - Increase and Promote IT Interaction with Mission
Strategy 1.1.1 - *Employ joint requirements generation processes and products to identify IT needs*. DoD conducts joint mission assessments and analyses, in a systematic, disciplined manner using uniform methods, to identify warfighting mission and support objectives, measures, architectures, and strategies including IT requirements. IT professionals are full partners in the assessment processes. IT requirements and solutions become an integral part of DoD IT architectures and plans linked to the DoD mission. ***(OPR= DoD CIO/JS, PPBS= RTA)***
Strategy 1.1.2 - *Influence and participate in operational exercises and demonstrations*. Build on the Joint Battle Center and Joint Warfighting Interoperability Demonstrations to (a) test and validate new IT concepts and technologies with end users, (b) increase the focus on end-to-end, interoperable capabilities that integrate warfighting and support activities, (c) explore leading edge concepts, Internet solutions, advanced commercial technologies, reengineered processes, and industry ìbest practicesî in DoD mission scenarios, and (d) exploit combinations of ìliveî environments and simulation models to reduce cost and increase flexibility. ***(OPR= DoD CIO/JS, PPBS= RTA)***

Objective 1.2 - Serve Mission Information Users as Customers
Strategy 1.2.1 - *Promote quick, easy user identification of information products and services.* Customers will have a menu of mission/task related products, services and related cost/performance. Develop and use a ìcustomer - supplierî model in IT support architectures, systems, processes, and operational procedures. Ordering information support services, and IT products should be as simple as ordering power from a utility or phone services from the telephone company. ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 1.2.2 - *Build a framework to determine the value of information.* Our military capabilities are heavily dependent on focused information. The value of information is a primary discriminator in business decisions, e.g. Return On Investment (ROI), and information assurance protection strategies. Methods and tools to help a customer determine information value are needed to explore new approaches in the way we manage our information resources. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 1.3 - Facilitate Process Improvement
Strategy 1.3.1 - *Promote and institutionalize methods to improve mission processes.* Major improvements are recognized by using process reengineering disciplines to rigorously analyze processes and relate those to mission. However, order of magnitude improvements are recognized by integrating processes across current stove-pipes. The initial target is to get a core set of consistent process models necessary for analysis of potentially high payoff, cross functional opportunities. ***(OPR= DoD CIO/JS/PSAs, PPBS= AIS)***
Strategy 1.3.2 - *Align IT investment decisions to support improved business processes.* To support improved processes, IT alternatives must consider mission impacts (e.g., Return-on-Investment) at the DoD-wide, functional, and organizational levels. Comparative sources for efficiencies include IT benchmark services and costs, best practices, consolidate capabilities, standardize systems, and share resources. ***(OPR= DoD CIO/ Component CIOs, PPBS= AIS)***

GOAL 2

Provide services that satisfy customer information needs



Description: The DII Master Plan identifies the major elements of the information infrastructure, roles and responsibilities, and serves as a tool to track the evolution of the DII into a service environment. To meet its global mission, DoD must focus the information infrastructure on getting information to mission and mission support customers from multiple information suppliers/providers. Today's systems are too often narrowly focused, not fully interoperable, and support a single function or organization requiring users to assemble information from incompatible sources. As information generation capabilities become more complex (e.g. maps, pictures, correspondence) DoD must begin to manage the information space for the user, and integrate and modernize its information infrastructure. Users need "navigation" services to leverage new technologies and information resources to retrieve, fuse and format information quickly. Accelerating the establishment of a network of shared databases and focusing the use of Internet technologies will support the ability of users to get information they want and reduce redundancies in stovepiped systems. A common operating environment throughout DoD from installations to weapon system platforms will expedite application system implementation and allow incremental implementation. Infrastructure components must move from an "organization/technology centric" paradigm to an interconnected set of services/products with quantifiable cost and performance measures to determine value-added to the mission.

Outcome: Users get mission oriented information and interoperable information technology services to satisfy their requirements easily and in a timely manner, anywhere in the world. Infrastructure planning ensures that long lead time items such as new technologies, capacity, facilities, and contracts are available when needed. Services, costs, and performance information are visible at all levels for objective decision making. DoD IT service delivery compares favorably with world class benchmarks in both cost and performance. Information sources, systems, and facilities (outsourcing, COTS, etc.) are transparent to the user.

Outcome Performance Indicators:

1. Customer satisfaction surveys and assessments,
2. Generic service performance measures for parameters such as cost, schedule and response time,
3. Self-assessment "maturity" models for information infrastructure elements such as software development, program management, megacenter management, network management, and base infrastructure,
4. Assessments for evaluating compliance with policy and standards such as Year 2000, Technical Architecture Framework for Information Management (TAFIM), Defense Information Infrastructure Common Operating Environment (DII/COE), and Joint Technical Architecture (JTA).
5. Government and industry quantitative benchmarks for equivalent IT products and services.

Primary Performance Evaluation Office(s): Military Departments (MILDEPs) and Defense Agencies

Models of Excellence:

DoD: Global Command & Control System (GCCS), DII Common Operating Environment (COE), Information Dissemination Management (Bosnia C2 Link)

DoD Presidential Quality Award Winners: Defense Mapping Agency (now National Imaging and Mapping Agency (NIMA))
Industry National Baldrige Award Winners: AT&T Network Systems Group

---

Objective 2.1 - Build Architecture and Performance Infrastructures

Strategy 2.1.1 - *Deploy a comprehensive, uniform methodology to define and integrate DoD architectures*. Architectures provide the best, long-term definition of the mission and related IT support. An integrated architecture framework for operational, systems and technical architectures must be established ensure interoperability and consistency. A disciplined support environment, similar to that provided by "data modeling" support tools, would advance a common understanding of missions and IT support by enforcing rigorous element definitions and relationships to other elements. Roles and responsibilities for generating, integrating, and using architectures in managing information and supporting IT must be institutionalized. The Architecture Coordinating Council co-chaired by Assistant Secretary of Defense (Command & Control, Communications, and Intelligence) (ASD(C3I)) and Undersecretary of Defense (Acquisition & Technology) (USD(A&T)) can be a catalyst. The target is a "system of systems" architecture for C4ISR and IT that can be expanded to include other missions. Interoperability must be "built-in" throughout the process, from requirements generation through certification and testing. and demonstrated in "live" environments like the Joint Battle Center (JBC) ***(OPR= DoD CIO/PSAs, PPBS= RTA)***

Strategy 2.1.2 - *Build performance management into the infrastructure*. The DII Master Plan must be extended to include products, services, and performance measures for each DII element. When complete, efficiency and investment decisions can be based on systematic assessments of information cost and value added to mission customers. Fielding a user oriented performance management system to systematically capture, archive, and report performance information. ***(OPR= DoD CIO/DISA, PPBS= C&CI)***

Objective 2.2 - Modernize and Integrate Defense Information Infrastructure

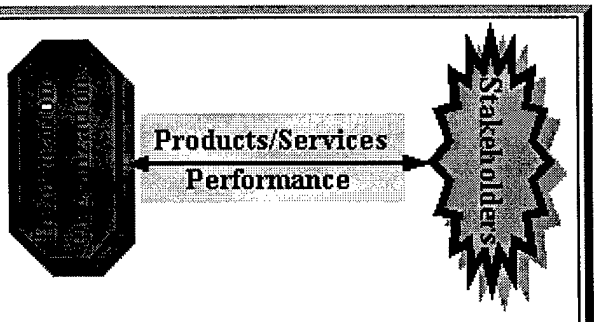
Strategy 2.2.1 - *Improve base level infrastructure*. DoD's base level communications and computing infrastructure needs to be reengineered and upgraded. Inconsistencies in technical and management procedures and capabilities complicate IT change planning and implementation. A major effort will be required to put in place a consistent management structure and modernized IT able to deliver quality support. The initial target date is to complete reengineering of primary mission critical bases and modernize their IT to levels needed to support joint operations. ***(OPR= DoD CIO/Component CIOs, PPBS= C&CI)***

Strategy 2.2.2 - *Continue migration system implementation*. As migration systems align applications support with DoD functions and processes, future IT investments can be linked directly to process improvements. Migration systems must have plans to achieve acceptable levels of JTA/COE compliance by 2002 or earlier. Continued emphasis must be placed on implementing systems to support reengineered processes that achieve mission and functional goals and measures of performance. Information support providers, in house and contractors, must maintain a program of continual improvement keyed to user requirements, software best practices, and the software capability maturity models. ***(OPR= DoD CIO/.PSAs, PPBS= AIS)***

Objective 2.2 - Modernize and Integrate Defense Information Infrastructure (cont'd)
Strategy 2.2.3 - ***Expedite shared data environment implementation***. Sharing data is a key to interoperability and quality data. Requirements are exploding for reliable, secure, efficient shared information repositories to support migration systems data and World Wide Web (WWW) information. Core mission critical data items must be logically organized and shared under the control of data "stewards" who are responsible for their quality and use. The target is a DoD-wide, accessible repository with enough critical information (e.g. 2000 core data items) to support DoD operations. Private facilities and sources should be assessed when considering alternatives. ***(OPR= DoD CIO/PSAs/DISA, PPBS= C&CI)***
Strategy 2.2.4 - ***Expedite implementation of common standards.*** JTA/COE provides the standards and interface environment for interoperability and a transparent technical infrastructure that supports all applications. Wide implementation will reduce planning time for applications and enable their timely, incremental implementation in a "plug and play" environment. Infrastructure elements and applications should be JTA/COE compliant at appropriate levels by the year 2002 or earlier. ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 2.2.5 - ***Fix year 2K problem.*** The objective is to experience no disruption at the turn of the century and have capabilities to respond quickly to residual errors. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 2.3 - Upgrade Technology Base
Strategy 2.3.1 - ***Rapidly insert advanced technology to support the mission***. Technology is changing faster than the infrastructure can adapt. New methods are needed to gracefully introduce new technologies incrementally with manageable risk rather than requiring lengthy contracting and development efforts. Current approaches such as the JBC, Advanced Concept Technology Demonstrations (ACTDs), Advanced Warfighting Experiments (AWEs) and Joint Warfare Interoperability Demonstrations (JWIDs) must be integrated, expanded, and fully exploited to meet this challenge. Distributed, Internet environments must be used to assess, test, integrate, and acquire new IT capabilities and COTS products. The target date is a systematic management structure and methodology that ìpipelinesî new technologies linked to evolving mission needs, and smoothly supplies these capabilities to the field. ***(OPR= DoD CIO/DISA/ARPA, PPBS= RTA)***
Strategy 2.3.2 - ***Move to an information service paradigm.*** Building on the Bosnia C2 Link experience, the Information Dissemination Management (IDM) concept provides a collaborative environment to help a user find information from a variety of sources known to the infrastructure but not the user. Defense Information Systems Agency (DISA) and Advanced Research Projects Agency (ARPA) are exploring automated user assistance mechanisms based on search and artificial intelligence techniques. IDM requires a new concept of operations for information and new support structures (e.g., information cells in theater staffed by military mission experts and IT professionals). The target is to institutionalize the Bosnia Link successes in all theaters capable of supporting emerging contingencies or crises. Simplifying requirements detail and reducing lead times for new information requests should achieve near-real-time response for warfighters and world class response for support environments. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 2.4 - Improve IT Management Tools
Strategy 2.4.1 - ***Model and simulate the integrated information infrastructure.*** A simulation model of the DoD IT infrastructure (the DII and user services) is needed to address cost, capability and performance over time for all infrastructure elements (e.g., communications, processing, data), and links to the mission. Existing models of DII segments and the DII Master Plan elements provide a starting point. The target is to provide comprehensive insight allowing CIOs and other decision makers to systematically evaluate personnel, service, cost/performance, acquisition, and operational issues and impacts. ***(OPR= DoD CIO/DISA, PPBS= RTA)***
Strategy 2.4.2 - ***Integrate information access and management methods for all media and types of information.*** The user needs automated, streamlined methods to routinely and reliably access information. A common semantics, syntax, and procedures set would include electronic directories, such as Government Information Locator Service (GILS), the Defense Data Dictionary System (DDDS), and directory and search methodologies employed by WWW information providers. The target is for on-line data dictionaries to be a primary source for DoD user assistance when accessing information (e.g. WWW documents). ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 2.4.3 - ***Implement IT Total Asset Visibility (ITTAV) universally.*** Total Asset Visibility is a Defense-wide initiative. The ITTAV concept can be used to manage IT ìobjectsî like hardware, software, and data for the user throughout their life-cycle. ITTAV "tracking" includes tracking the status of user orders for information objects, maintaining accurate inventory records, automatically ordering upgrades, and managing asset reuse and removal. The target is a WWW based repository that can be accessed by developers and users to determine availability, reliability, maintainability, etc., for any information or IT asset affecting their service. The repository should include information maintained by the Defense Integration Support Tool (DIST) and the Automation Resources Management System (ARMS), and use standards and procedures compatible with JTA/COE and Electronic Commerce /Electronic Data Interchange (EC/EDI). ***(OPR= DoD CIO/Component CIOs, PPBS = RTA)***

GOAL 3 ***Reform IT management processes to increase efficiency and mission contribution***	

Description: As resources decline, information and information technology must be managed as a strategic resource, from a DoD-wide perspective. DoD must base information and information technology decisions on their contribution to the effectiveness and efficiency of military missions and supporting business functions. It is important to manage IT resources, and align strategies and programs with Defense-wide, functional, and organizational goals and measures. Information technology management, itself a business function, must employ best business practices to continuously improve customer/user support, reduce costs, and apply the best available information technology.

Outcome: IT organizations, DoD and commercial, are accountable to their stakeholders for their cost and performance and contribution to their organization's overall mission. Also, each IT organization shows continual improvement in quality and efficiency through regular assessments and attentiveness to best practices and benchmarks. Activities at all levels can quantify mission contribution of IT

investments to improved mission performance that withstands comprehensive audit. DoD Components can successfully articulate and defend IT investment funding with full accountability.

Outcome Performance Indicators:

1. Results of internal and external audits indicate compliance with laws and policy.
2. Organizational improvements can be assessed by the Presidential performance and results methodology (Baldrige criteria) supplemented by maturity models. (DoD Component CIOs will maintain performance status information by activity for categories such as current status, assessments completed, improvement plans in place and funded.)
3. Effective use of resources is evaluated by customer surveys and demonstrated ability to obtain resources for IT investments.
4. Evaluation of method and tool effectiveness can be assessed through customer surveys.
5. Personnel quality improvement can be measured by using formal certification methods for critical skills.
6. Quantitative improvements in ITM Strategic Plan goals/strategies using Plan measures.

Primary Performance Evaluation Office(s): DoD Chief Information Officer

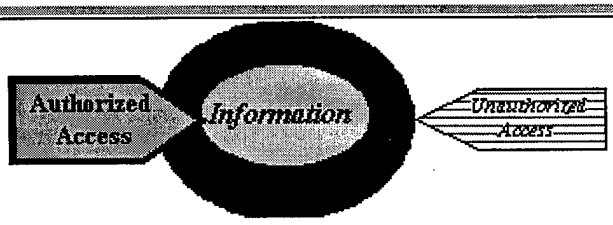
Models of Excellence:

DoD GPRA pilots: Defense Logistics Agency (DLA), Commander in Chief, Atlantic Fleet (CINCLANTFLT), Defense Commissary Agency (DeCA)
Industry National Baldrige Award Winners: AT&T, Ritz Carlton, Dana Commercial Credit, McDonnell Douglas Corp. (C-17 program)

Objective 3.1 - Institutionalize ITMRA Provisions
Strategy 3.1.1 - *Streamline IT planning and investment process*. ITMRA legislative direction allows new flexibility in managing IT coupled with accountability. This ITM Strategic Plan will guide all DoD IT activities. DoD Component ITM strategic plans and investment portfolio processes must be instituted to proactively lead the linkage of IT to the mission starting with joint mission assessments and analyses (see related Goal 1, strategy 1). The goal is for the CIO, Chief Financial Officer (CFO), and DoD Component CIOs to publish an annual report in 1999 that displays quantitatively improvements in all ITM strategic plan goals. To accomplish that goal the CIO Council and CIOs would demonstrate leadership to effect cross functional tradeoffs and infrastructure investments. ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 3.1.2 - *Institute the customer/user focus*. Tools and policy will help activities systematically introduce and maintain customer awareness and compare their performance with peers. In industry, customer focus is routinely practiced and supports continuous improvement of processes, practices, and people. Routine use of customer surveys by IT organizations at all levels is the target. ***(OPR= DoD CIO/Component CIOs, PPBS= RTA)***
Strategy 3.1.3 - *Make better, quicker outsourcing decisions*. Guidelines and a framework for systematically making outsourcing, privatization, and in-house decisions are needed at all levels. Policy and procedures are needed to address issues such as IT outsourcing and privatization scope and context definitions, expectations and targets, elements of acceptable business case analyses, and use of these in oversight and resource allocation processes. ***(OPR= DoD CIO/PSAs/Component CIOs, PPBS= RTA)***
Strategy 3.1.4 - *Improve acquisition processes.* Streamlined acquisition regulations and oversight processes can reduce acquisition overhead and lead time. Acquisition reforms should be fully implemented at all levels. Promising concepts and technologies from research experiments, pilot projects, and operational demonstrations must be moved through the acquisition process smoothly and efficiently. New paradigms of acquisition must be exploited that expedite the use of COTS (e.g., the Federal Acquisition Regulation (FAR) Section 12, new testing rules for COTS), reduce cost and lead time, and maintain interoperability. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 3.2 - Institute Fundamental IT Management Reform Efforts
Strategy 3.2.1 - *Improve IT management processes* - A comprehensive reengineering of IT processes will serve to identify the optimum collection of information needed for efficient IT management. OSD, DISA, Army, Marine Corps and other existing models provide a substantive baseline. Experience in the IT community can be exported to produce cost/performance gains and cross-functional optimization in other areas. ***(OPR= DoD CIO/Component CIOs, PPBS= RTA)***
Strategy 3.2.2 - *Establish uniform organizational measure and assessment processes.* Performance measures linked to mission needs to be embedded systematically at all levels of DoD including local activities and IT staffs. Capability Maturity Models (CMM) for software development and Baldrige Award Criteria are widely accepted as effective organizational improvement methods, private and public. While the focus is on organizational improvement, both CMM and Baldrige provide a quantitative assessment method that can be used as a performance indicator. The target is for DoD IT organizations to routinely publish performance information including customer satisfaction results and regularly report formal maturity level assessments for IT support. ***(OPR= DoD CIO/Component CIOs, PPBS= RTA)***
Strategy 3.2.3 - *Improve methods and tools* - Tools have been provided to assist activities performing BPR, benchmarking, TQM, and other improvement activities. These and other tools must be integrated into the actual life-cycle, so end-users, managers and developers can apply them easily, routinely, and incrementally and also share results with others. Expansion is needed to make the capabilities available via WWW and useful for integrating with other DoD systems, including regular reporting. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 3.3 - Upgrade DoD IT Workforce
Strategy 3.3.1 - *Provide training and educational opportunities.* Ensure that ITM processes, policies and innovations are supported by appropriate training, professional development, and rewards for the work force of the DoD. ***(OPR= DoD CIO/Component CIOs, PPBS= RTA)***
Strategy 3.3.2 - *Effectively utilize current personnel processes.* Use the recruitment process, to acquire skilled personnel based on ITM Core Competencies. Use the performance evaluation process to assess employee performance to determine required training in areas that are determined to be deficient. ***(OPR= Component CIOs, PPBS= RTA)***
Strategy 3.3.3 - *Use organization and individual assessment tools* to determine skill requirements. For example, the People Capability Maturity Model developed by Software Engineering Institute (SEI) could provide a systematic method of assessing organizational requirements for local use and to identify knowledge and skill gaps for management at all levels. ***(OPR= Component CIOs, PPBS= RTA)***

GOAL 4 ***Ensure DoD's vital information resources are secure and protected***	

Description: Our vital information resources and information infrastructures are at risk. These

infrastructures must be available to provide authentic and accurate information, and have protection and resiliency against information warfare, and terrorist and criminal activities. Assuring absolute security is not feasible. DoD must protect systems by exercising a well-analyzed risk management approach, augmented by efforts to detect unauthorized access or intrusions into systems. This approach must be supported by plans and resources that respond to these occurrences including provisions for restoring critical services and systems in a priority manner when disruptions are successful.

Outcome: DoD information resources and systems are protected against information warfare and other threats, whether they arise from traditional military conflicts, terrorism, criminal activity, or misuse. Risk mitigation capabilities anticipate and prevent incidents, and rapidly respond to restore critical services in a priority manner. Quality products and services are available to provide a range of options tailorable to user needs.

Potential outcome indicators::

1. Penetration attempts detected and repelled,
2. Degree of application of strong identification and authentication (I&A), trusted systems, and Multilevel Information Systems Security Initiative (MISSI) components for system protection,
3. Compliance with DoD security policies and recommended security practices as evidenced by GAO audits and Inspector General (IG) investigations,
4. Deficiencies identified during exercises and assessments

. **Primary Performance Evaluation Office(s):** Office of the Deputy Assistant Secretary of Defense (Command, Control & Communications / Information Assurance)

Models of Excellence: TBD

Objective 4.1 - Build Information Assurance Framework
Strategy 4.1.1 - *Keep DoD personnel current.* Provide improved awareness, training, and professional development for users, managers, and administrators related to information assurance issues. ***(OPR= DoD CIO/Component CIOs, PPBS= RTA)***
Strategy 4.1.2 - *Establish policy framework.* Update or establish new DoD policies that will provide the policy framework for Department's Information Assurance efforts. ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 4.1.3 - *Provide guidance.* Provide risk management guidance and practices to be applied for managing risks applicable to DoD systems. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 4.2 - Build Information Assurance Architecture and Supporting Services.
Strategy 4.2.1 - *Build information assurance architecture.* Assure DoD architectures include required elements, and identification of applicable standards to assure consistency needed for an infrastructure centered view of information assurance. ***(OPR= DoD CIO/DISA, PPBS= RTA)***
Strategy 4.2.2 - *Integrate COTS products*. Leverage interaction with and commercial-development and use of protection and other products and services that have been endorsed as compliant with DoD needs. ***(OPR= DoD CIO, PPBS= RTA)***
Strategy 4.2.3 - *Establish security infrastructure services*. Common Department-wide services, such as public key infrastructure and directories, assure availability and minimize duplication. ***(OPR= DoD CIO, PPBS= RTA)***

Objective 4.3 - Improve Acquisition Processes and Regulations
Strategy 4.3.1 - *Update acquisition regulations*. Work with the DoD acquisition community to strengthen the acquisition process and procedures to improve the information assurance posture of existing and future systems, information, and components. ***(OPR= DoD CIO/USD(A&T), PPBS= RTA)***
Strategy 4.3.2 - *Employ System Security Engineering Capability Maturity Model (SSE-CMM).* Use the model in contract evaluation and selection processes and when upgrading current capabilities. Work with the industry's SSE-CMM Steering Committee to foster CMM efforts, which is similar to software capability model efforts for security design and integration. ***(OPR= DoD CIO/USD(A&T), PPBS= RTA)***

Objective 4.4 - Assess Information Assurance Posture of DoD Operational Systems
Strategy 4.4.1 - *Continue online security assessments* . Establish required policies and standardization and encourage Departments and Service to do self assessments on a continual basis to uncover weaknesses and vulnerabilities in their systems that can be exploited by outside and inside attackers. *(OPR= DoD CIO/ Component CIOs, PPBS= RTA)*
Strategy 4.4.2 - *Perform "information operations (IO) red teaming"* Institutionalize a "red team" process to assess critical systems throughout their life-cycle and operations readiness, especially during military exercises. *(OPR= DoD CIO/ Component CIOs, PPBS= RTA)*

V. Making It Happen

The DoD ITM Strategic Plan is a key part of an end-to-end strategic planning process designed to guide DoD Components in performing their ITM strategic planning and implementation activities. OSD Principal Staff Assistants (PSAs) and the Joint Staff formulate their guidance for improving mission performance within each functional area and activity. The ITM Strategic Plan integrates management requirements across functional areas and missions into cross-cutting thrusts and initiatives supporting the Department as a whole. DoD Components use this guidance to prepare their plans and programs in support of their unique missions and to execute assigned DoD-wide initiatives. Performance guidance is applicable at all DoD levels.

ITM Strategic Planning Process

This section describes the ITM strategic planning cycle. While this cycle is aligned with the PPBS, its influence extends beyond the formal planning, programming, and budgeting system into all information related activities. The primary purpose is to establish an IT management structure and process to improve IT support to the mission and successfully defend IT investments by demonstrating mission improvement. The ITMRA requires an annual report be submitted with each budget showing actual results based on a strategic plan.

The ITM strategic planning process includes:

DoD Component Strategic Planning. Each DoD Component will maintain a DoD Component ITM strategic plan consistent with the DoD ITM Strategic Plan. DoD Component strategic plans will inherit the DoD goals and strategies and identify supporting initiatives. Additional sections may be added to identify performance gaps, specify additional goals, objectives, and supporting strategies. Actions to support formal goals and strategies can expect review and support from the DoD CIO during PPBS processes. DoD Component strategic plans will include their IT investment criteria and portfolio decision process.

Performance and Assessment. Strategic goals and strategies will be governed by formal performance measures as a routine management practice. Appendix D identifies performance and assessment guidance developed and maintained in coordination with DoD Components. A "Primary Performance Evaluation Office" is designated for each goal and a "Office of Primary Responsibility" (OPR) for each strategy. Those offices will oversee definition of performance indicators, data gathering and reporting of results. DoD Component strategic plans will show how they support and contribute to the achievement of DoD-wide measures and targets and make performance information available. The annual report to the CIO council will report the actual performance results for their review. (*The initial measure procedures, baselines, and targets will be established as a near-term action.)*

Near-Term Actions. Appendix E contains near-term actions necessary to pursue objectives and strategies to accomplish Section IV goals.

The strategic planning and annual report cycle is keyed to CIO Council meetings and linkage with DoD Component planning processes and OSD PPBS schedules. Actions include approving DoD ITM strategic plan, implementing near-term actions, reviewing planning and resourcing problems and opportunities, measuring performance and developing and approving annual report(s). Review for the annual report will be accomplished concurrent with strategic plan update including performance and near-term action appendices.

Strategic Plan Interaction with PPBS

The ITM strategic plan can be an important contributor to the PPBS process and products. The top level goals and strategies provide a common, coordinated basis for input to the other Defense planning and detailed guidance for DoD Components.

DoD Component CIOs have a critical role in ensuring DoD ITM goals and strategies are supported in DoD Component plans and program/budget inputs. The guidance in the DoD ITM Strategic Plan will be a common basis for developing DoD Component strategic plans. The combination of DoD and DoD Component plans will support DoD Component investment decision making during their program build processes and justify programs at the DoD level.

The ITM Strategic Plan is a basis for identifying issues for OSD program review. The adequacy of resources programmed to support DoD ITM strategies and measures of performance will be assessed. Approved Program Objective Memoranda (POM) make adjustments at the OSD level in the Future Year Defense Program (FYDP) submitted to OMB and Congress. In addition, significant strategic plan issues may necessitate "out-of-cycle" Program Budget Decisions (PBDs), adjustments to the current budget year.

References

Association for Federal Information Resources Management, *The Federal Chief Information Officer, Top Ten Challenges Survey,* October 1996
Clinger-Cohen amendment to the National Defense Authorization Act of 1996, *Information Technology Management Reform Act (ITMRA)*
Defense Information Systems Agency, *Defense Information Infrastructure Master Plan,* April 1996
Department of Commerce, *Malcolm Baldrige National Quality Award, 1997*
DoD Directive 8000.1 - Defense Information Management (IM) Program
DoD Directive 5000.1 - Defense Acquisition
DoD Regulation 5000.2-R - Mandatory Procedures for MDAP and MAIS Acquisition Programs
Executive Order 13011 of July 16, 1996, *Federal Information Technology (ITMRA Implementation)*
The Federal Acquisition Reform Act of 1996 (FARA)
Federal Acquisition Streamlining Act of 1993 (FASA)
The Government Performance and Results Act of 1993 (GPRA)
Chairman, Joint Chiefs of Staff, *Joint Vision 2010*
National Academy of Public Administration, *Information Management Performance Measures,* Washington DC, January 1996.
Office of Management and Budget Circular A-11, Part 2 - *Preparation and Submission of Strategic Plans*
Office of Management and Budget Circular A-11, Part 3 - *Planning, Budgeting, and Acquisition of Fixed Assets*
Office of Management and Budget Circular A-130 - *Management of Federal Information Resources*
Office of Management and Budget, Memorandum to Heads of Executive Departments and Agencies, Subject: *Funding Information Systems Investments,* October 25, 1996
Office of the Secretary of Defense (C3I), *Guide for Managing Information Technology (IT) as an Investment and Measuring Performance,* February 1997
Paperwork Reduction Act of 1995 (PRA)
Principal Deputy Undersecretary of Defense (Comptroller), *DoD Implementation of Government Performance and Results Act (undated).*
Report of the Federal CIO Working Group to the Office of Management and Budget, July 1996
Secretary of Commerce, *Malcolm Baldrige National Quality Award, Profiles of Winners,* (current version on WWW)

List of Acronyms

TERM	EXPANSION
A&T	Acquisition & Technology - OSD office
ACTD	Advanced Concept Technology Demonstration
AIS	Automated Information System
ARMS	Automation Resource Management System
ARPA	Advanced Research Projects Agency
ASD	Assistant Secretary of Defense
AT&T	American Telephone & Telegraph
AWE	Advanced Warfighting Experiments
BPR	Business Process Reengineering
C&CI	Communications & Computing Infrastructure
C2	Command & Control
C3	Command, Control, & Communications
C3I	Command & Control, Communications, and Intelligence
C4ISR	Command & Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
CINC	Commander in Chief
CINCPACFLT	Commander in Chief, Pacific Fleet
CINCSTRATCOM	Commander in Chief, Strategic Command
CIO	Chief Information Officer
CMM	Capability Maturity Model
COE	Common Operating Environment
COTS	Commercial Off-the-Shelf
DDDS	Defense Data Dictionary System
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DIST	Defense Integration Support Tool
DoD	Department of Defense
DSC	Defense Decision Support Center
DUSD	Deputy Undersecretary of Defense
EC	Electronic Commerce
EDI	Electronic Data Interchange
FAR	Federal Acquisition Regulation
GAO	General Accounting Office
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GPRA	Government Performance and Results Act (of 1993)

TERM	EXPANSION
I&A	Identification & Authentication
IA	Information Assurance
IBM	International Business Machines Corp.
IDEF	Integrated Definition Modeling methodology
IDM	Information Dissemination Management system
IG	Inspector General
INFOSEC	Information Security
ISO	International Standards Organization
IT	Information Technology
ITM	Information Technology Management
ITMRA	Information Technology Management Reform Act
ITTAV	Information Technology Total Asset Visibility
JBC	Joint Battle Center
JTA	Joint Technical Architecture
JWID	Joint Warfare Interoperability Demonstration
MILDEP	Military Department
MISSI	Multilevel Information Systems Security Initiative
NSS	National Security System
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OTS	Off the Shelf
PBD	Program Budget Decision
POM	Program Objectives Memorandum
PPBS	Planning, Programming, and Budgeting System
PPI	POM Preparation Instructions
PRA	Paperwork Reduction Act (of 1995)
PSA	Principal Staff Assistant (to the Secretary of Defense)
ROI	Return on Investment
RTA	Related Technical Activities (See Tab G of the OSD POM Preparation Instructions (PPI).)
SEI	Software Engineering Institute (of Carnegie Mellon University)
TAFIM	Technical Architecture Framework for Information Management
TQM	Total Quality Management
USD	Undersecretary of Defense
WWW	World Wide Web

Appendix A - Guiding Principles

This Appendix captures essential elements of the ITMRA, DoD Directive 8000.1, presidential quality award management principles, and the National Defense Performance Review objectives. They identify general management improvement tenets and initiatives which impact formulation of ITM goals and objectives.

Strategic Planning Guidelines

1. ***Improve defense processes.*** Employ business reengineering practices, methodologies and tools to the develop or refine processes before system automation is undertaken. New business methods and procedures are proven and validated in pilot projects before organization-wide implementation. Information technology services are engineered to optimize process outputs (products and services), and outcomes (expectations and knowledge).
2. ***Take a user/customer focus.*** Information will be managed so it improves the understanding of how to effectively provide user services so that informed choices can be made by providers and beneficiaries based on the recognition of best value. Quality, interoperability and timeliness defined in terms of end user or process, not succession of interfaces.
3. ***Tightly couple ITM with mission/user requirements.*** The warfighter knows the job to be performed and information needs. ITM service providers must be immersed in the mission and user environments to be able to communicate clearly the options available and anticipate future needs to put in place long lead time items.
4. ***Ensure information is secure and available to authorized users.*** Knowledge must be protected from attack and misuse, while at the same time being easily available to users who need it to perform their tasks. Our reliance on information must not be turned against us. IM capabilities must be sufficiently resilient, redundant and fail-safe to ensure continuity of operations under traditional and emerging threats. Catastrophic failures in our global information grid could present our adversaries with an "information Achilles heel."
5. ***Promote accountability.*** Programs and resources will be aligned to joint requirements and priorities and implemented through strong cost and performance linkages with the PPBS processes at all levels. Accountability for product and service cost and performance measures goal accomplishment at each level, replacing hierarchical models.
6. ***Integrate commercial capabilities***. Tremendous life cycle savings can be recognized by capitalizing on commercial products and services. Changing processes to accommodate "off-the-shelf" products and services need to be considered and balanced with DoD development, deployment, training and support costs. Critical skills, knowledge, and capabilities must be mobilized to support defense missions in military, civilian, and/or industrial organizations. Outsourcing functions and employing COTS products and services frees resources for application to unique DoD missions.
7. ***Foster learning, collaboration and empowerment.*** Our processes must motivate and reward our military and civilian personnel and industry partners to act from a joint, Defense-wide perspective to realize our shared vision for the future. We must become a learning organization, work as a team, and empower people to achieve excellence in meeting future defense challenges. Self assessment instruments articulate policy and doctrine at the job/organization level, eliciting understanding and accountability, replacing extraneous oversight and reporting.
8. ***Achieve the required degree of interoperability***. Interoperability must be measured on an end-to-end basis. End users must understand and use the information presented. Further, we must be able to share and use knowledge and capabilities jointly and with our allies and coalition partners to the degree necessary to meet mission needs. Our capabilities must transcend a single language and ensure a common understanding as the basis for working and winning as a joint and combined force.
9. ***Exploit models and architectures.*** Process and data models and various architectures define information requirements and guide support strategies over the long-term (5-10 years). Efforts must use approved architectures, and formal methods available to evolve them through use of change requests. We must replace hardware and software based management with doctrinally-driven operational requirements, captured in architectures, translated into capabilities

that are responsive to information needs and changing missions and doctrine.

10. ***Demand adaptable, innovative, incremental, and modular approaches and solutions.*** Capabilities must be tailorable, scaleable, and configurable, so that the right "package" of capabilities can be assembled, integrated, and applied to each unique contingency and crisis. In the field, capabilities must rapidly adapt to the full range of operational conditions, new situations and technologies without complete redesign. Our processes and practices must become more innovative, while maintaining a focus on a shared vision. Modernization and contracting efforts will employ incremental, modular strategies to reduce risk and increase responsiveness to user requirements and transparently introduce new technologies. These must be accomplished in a compressed time frame to minimize the cost of development and achieve early realization of benefits.

Implementation Planning Guidelines

1. ***Build on current programs and capabilities.*** The seeds for achieving the strategic goals are now emerging. These should be fully exploited wherever possible. Examples include Joint Vision 2010 and other Strategic Plans, Defense Information Infrastructure (DII), Common Operating Environment (COE), Global Command and Control System (GCCS), Global Combat Support System (GCSS), C4ISR Report and Mission Area Assessment, Process Improvement projects, Total Quality Management efforts, Government Performance and Results pilots, Modeling and Simulation, Migration Systems and the Information Assurance Program.
2. ***Maintain current program and operations assessments.*** Linking projects and programs to strategies and measures provides a basis for determining funding levels and go/no go decisions.
3. ***Move to product/service/performance based structures.*** Management techniques emerging from GPRA pilots and ITMRA policies describe our organizations and support structures in terms of processes, outcomes, products and services, and customer expectations. Customer decision cycles drive management decisions and efficiencies are determined by comparing unit performance with the best government or industry benchmarks. Architectures, interoperability, and acquisitions are measured in terms of end-to-end product/service rather than infrastructure component performance.
4. ***Help people adapt.*** Performance based organization concepts emphasize collaboration, teamwork, customers, and services/production. This is a major change for the DoD. Jobs are defined by tasks depending on a mix of knowledges and skills as much as organization position. Basic values such as identity, loyalty, security, and interpersonal relationships change and need to be reinterpreted. Education and training move to incremental and "just in time" strategies. These "cultural" transitions often dictate the pace of accomplishing the other objectives.
5. ***Promote senior management involvement.*** Senior managers must understand, adopt and promote strategic objectives. Performance based organizations assume agility and change based on trust and openness to discover how organizations work together to provide end-to-end service to customers. Current systems reward building and maintaining stove-piped organizations that can stalemate innovation and destroy teamwork.
6. ***Couple mid-term and long-term goals with near-term actions.*** Strategic plans must set longer term goals to guide and synchronize major efforts but also identify near-term actions, start transitions, and gain credibility.

Performance Guidelines

1. ***Link to Strategic Planning.*** Wherever possible, performance measures should be linked to strategic planning missions, visions, goals, objectives, or strategies. Strategic plans provide the context to define individual measures and interaction between measures.
2. ***Engage stakeholders.*** Stakeholders are evident at each organizational level and can include (a) customers and suppliers -- current and future, (b) employees and support contractors -- current and future, (c) higher order management (e.g., headquarters, OSD, OMB, Congress), (d) subordinate organizations seeking guidance (e.g., headquarters-field, OMB-OSD, OSD-MILDEPs, etc.)
3. ***Empower the field.*** Empowerment means making the factors for incentives and disincentives of actions and decisions visible to all parties, precluding the need for oversight. Performance measures are a key methodology. Strategies and tools must allow local managers to define and

measure performance and results against stakeholder expectations.

4. ***Measure outcomes wherever possible.*** Measures are typically categorized as input, output, and outcome. Input measures are relatively easy to quantify and capture, e.g. resources, requests, students, etc. Output measures can be quantified for organizations with formal product and service descriptions but difficult for those with more abstract mission statements. Outcome measures of the vision or stakeholder satisfaction with products and services are multi-dimensional and hard to identify and quantify. However complex, outcome measures are the most valuable for decision making.
5. ***Focus on achievement.*** Measures are applied at many levels. A few, well chosen, outcome-oriented measures are better than multiple, potentially conflicting, sub-optimal measures. All efforts should be focused on one or more measures mutually arrived at in consultation with stakeholders.
6. ***Find trend indicators.*** Indicators will be selected to measure progress towards a particular goal or target. The user should be able to graph value with respect to time for quality, quantity, etc. For complex environments values will typically be represented as a "high-low-most likely" to represent the range of responses and preclude excessive description necessary to defend a single value. *Note that completion of an action is not a trend.*
7. ***Use widely accepted methods.*** The Baldrige criteria and Capability Maturity Models (CMM) are comprehensive, long-term, proven methodologies for improving organization effectiveness, including performance. They benefit from extensive discussion, application in a variety of environments, and frequent review and refreshment. Robust infrastructures of information, benchmarks, training, and experience is augmented by a culture of openness and sharing. Participation reduces personnel and financial investments and also lead time. International Standards Organization (ISO)-9000 standards, and various customer survey instruments are also available.
8. ***Make the "business case" for each measure.*** Performance measurement procedures have matured over time. Initial efforts often created apparently useful measures that proved ineffective because the the processes for gathering and using performance information were inadequately defined, the cost of gathering information outweighed the benefits, and user responses to the measure detracted from achieving the goal. Practitioners have identified templates to ensure effective measures are defined. Common questions that must be addressed include (1) What is the measure supposed to show? (2) Who measures and how? (3) Who uses and for what? (4) How could the measure be used to subvert or be misinterpreted (unintended consequences)? (5) How much will it cost to measure? (6) What is the estimated value to the user? (7) Are there any provisions such as tools and assistance that could help, and (8) Are there any critical factors that need to be considered?

Appendix B - Information Technology/Defense Information Infrastructure PPBS Reporting Structure (Tab G)

This Appendix contains information extracted from the current, draft Tab G of the OSD POM Preparation Instructions for reference purposes.

General Guidance

Purpose. This chapter of the POM Preparation Instructions deals with the programs and resources that are categorized as Information Technology (IT) activities, particularly the Communications and Computer (C&C) Infrastructure programs, the Functional Area Automated Information Systems (AISs), and the Related Technical Area initiatives that comprise the Defense Information Infrastructure (DII). The reporting required by this tab is intended to capture the entirety of the DoD's programmed consumption of IT resources as defined in the Information Technology Management Reform Act of

1996. In particular, information technology means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes computers, ancillary equipment, software, firmware and similar procedures, services, and related resources. This reporting will include activities categorized as National Security Systems (NSS) in the Information Technology Management Reform Act (ITMRA) of 1996 which are managed by this POM process.

Requirement. IT/DII resources have the potential to provide savings spread widely across the DoD. These resources require visibility and sound management to ensure that the C&C Infrastructure and Functional Area Automated Information Systems (AISs) being researched, developed, procured, deployed, modified, operated and maintained by the DoD are cost effective, sufficient, efficient, secure, and interoperable. The Related Technical Activities must be structured and applied across the DII to attain these ends. Although the information required by this tab is not the only input required to make well-supported decisions on information technology resource investments, it provides an overview of IT/DII resources and activities to be used by the Chief Information Officer (CIO) and the programming and budgeting communities to ensure high priority requirements are supported.

To assist in the management and decision processes and be responsive to legislation such as the Information Technology Management Reform Act (ITMRA), an Executive Summary (ES) identical to the IT 43 ES (except that it covers all of the POM years, not just CY, BY, and BY+1) will be submitted with the Tab G data formats. This ES will track from the President's Budget Submission and cover all IT resources. It will include: (a) a general description of the DoD Component's IT activities and how they support the DoD Component's mission; (b) major IT initiatives supported in the POM submission; and (c) an explanation of all major changes since the PB submission. The reporting formats for the FY 1999-2003 POM have been revised to include a narrative and capture more of the pertinent information about a program that is of interest to decision makers. At the same time, the revised TAB G submission should not impose a significant burden on the DoD Components, since it represents at most an update of information required for budget documents or other management reports.

A number of systems are reported in both Tab C and Tab G of the POM Submissions, (and potentially other Tabs). The level of detail varies between the reporting activities; therefore all submissions are required. It is the responsibility of the submitting activity to report consistently among these requirements. Specifically, individual system investment appropriations reported in detail at Tab C will be consistent with that reported at the more summary level in the G-1 format.

For reporting in Tab G, the IT/DII is divided into three primary areas:

- **Functional Automated Information Systems (AIS)**: Functional area applications or AISs are associated with all DoD mission areas-C2, Intelligence and combat support areas. They rely upon the information processing, common services, and transport capabilities of the Communications and Computing Infrastructure. Related technical activities provide the architectures, standards, interoperability, and information assurance that these systems require to operate effectively as part of the Defense Information Infrastructure. Although an AIS may serve more than one function, it is classified according to its predominate function.

- **The Communications and Computing Infrastructure (C&CI)**: The C&CI provides the information processing (computing) and transport services (communications) used by functional applications. DoD common services, including most of what has historically been categorized as "value-added services", are considered to be part of the C&CI this year. These common services are communications applications such as voice, data transfer (including EC/EDI), video teleconferencing, and messaging.

- **Related Technical Activities (RTAs)**: Related Technical Activities service the DoD C&CI and AISs. While these activities do not directly provide functional applications, data processing, or connectivity, they are required to ensure that the infrastructure functions as an integrated whole and meets DoD mission requirements. RTAs include information assurance, spectrum

management, development of architectures, facilitation of interoperability, and technical integration. RTAs could be considered as "overhead" services that are necessary to the DII.

Figure (B)-1 summarizes these three major areas and their subdivisions; this structure will form the basis for FY1999-03 Tab G reporting.

Figure (B)-1: IT/DII Reporting Structure

Functional Area Automated Information System (AIS)	Communications and Computing Infrastructure (C&CI)	Related Technical Activities (RTAs)
1. Civilian Personnel 2. Command and Control 3. Economic Security 4. Environmental Security 5. Finance 6. Health 7. Information Management 8 Intelligence 9. Logistics 10. Military Personnel & Readiness 11. Nuclear, Chemical and Biological (NBC) Defense Programs 12. Other 13. Policy 14. Procurement/Contract Administration 15. Reserve Affairs 16. Science and Technology 17. Systems Acquisition Management 18. Test and Evaluation	1. Common Infrastructure Applications Voice Systems Messaging systems Data transport and Networks Video Systems Network and Systems Management 2. Communications Infrastructure Long Haul/Wide Area Deployable/Tactical/Shipboard Base Level 3. Computing Infrastructure Main-frame Processing Mid Tier processing Super Computing Deployable/Tactical/Shipboard Computing 4. Office Automation	1. Data Administration 2. Information Assurance 3. Interoperability 4. Technical Activities Testing Engineering Architectures 5. Other

Format G-1 Preparation Guidance

(*Only paragraph linking to ITM Strategic Plan - other information deleted*)

ITM Strategic Plan Goal/Objective (Two Characters) First Character: Select the ITM Strategic Plan goal that is most directly supported by this program. Second Character: Select the most appropriate objective associated with the selected goal. The goals and objectives are listed in the ***(this)*** ITM Strategic Plan. *Goals described in the current ITM Strategic Plan are:*

1. Become a Mission Partner

2. Provide services that satisfy customer information needs.

3. Reform IT management processes to increase efficiency and mission contribution

4. Ensure DoD's vital information resources are secure and protected

Appendix C - Links to Strategic Information

This Appendix identifies strategic documents and associated efforts that need to be considered when conducting formal ITM Strategic Plan reviews.

DoD Component Strategic Plans	
DoD-wide	• DoD Strategic Plan • National Military Strategy *(http://www.dtic.mil/doctrine/jel/other_pubs.htm)* • Joint Vision 2010 *(http://www.dtic.mil:80/doctrine/jv2010/jvpub.htm)* • Defense Information Infrastructure Master Plan *(http://www.disa.mil/dii/diiexe/execsum1.html)* • Joint Technical Architecture (JTA) • Technical Architecture Framework for Information Management (TAFIM) *(http://www.itsi.disa.mil/cfs/tafim.html)*
Air Force	• VISTAS, Air Force Information Resources Management (IRM) Strategic Plan *(http://www.cio.hq.af.mil/docs/vistas.doc)* • HORIZON, Air Force C4I Vision *(http://www.sc.hq.af.mil/)*
Navy	• DON Information Technology Strategic Plan (1997-2001)
Army	
Defense Information Systems Agency (DISA)	• Information Resources Management (IRM) Strategic Plan (1996-2001) • Standards Based Architecture (SBA) WESTHEM Implementation • FY 1996-2003 DoD Data Administration Strategic Plan
Defense Logistics Agency (DLA)	• Information Resources Management (IRM) Strategic Plan (1996 DRAFT)
Joint Staff	• A Strategic Plan for the Joint Staff • The Military Critical Technologies List *(http://www.dtic.mil/mctl/)* • Chairman's Joint Vision 2010 Implementation Policy

Functional Strategic Information	
Civilian Personnel	• -
Command and Control	• C4ISR Integration Task Force Executive Report, November 1996
Economic Security	• -
Environmental Security	• -
Finance	• Chief Financial Officer Financial Management 5-Year Plan.
Health	• Military Health Services System, Information Management/Information Technology Strategic Plan - *(http://www.ha.osd.mil/main/pagsp.html)*
Information Management	• Information Technology Management Strategic Plan
Intelligence	
Logistics	• Department of Defense Logistics Strategic Plan (Edition 1996/1997) *(http://www.acq.osd.mil/log/mdm/lsp96.htm)* • A Mosaic of Support to the Warfighter (*http://www.acq.osd.mil/log/mosaic/report*)
Military Personnel & Readiness	• -
Nuclear, Chemical and Biological (NBC) Defense Programs	• -
Other	• -
Policy	• -
Procurement/ Contract Administration	• -
Reserve Affairs	• -
Science and Technology	• -
Systems Acquisition Management	• -
Test and Evaluation	• -

Appendix D - Performance and Assessment

This Appendix defines the context, detailed guidance, and examples for measuring achievement of strategic planning goals, outcome performance indicators, and specific strategy related objectives and indicators of progress in this Plan.

Performance Requirements

The DoD CIO will ensure that performance measures are implemented for each strategy and goal. The Primary Performance Evaluation Office identified for each goal in section IV will assist in developing a set of outcome performance indicators, targets, and how the measures are used to improve national defense. The office of primary responsibility (OPR) listed for each strategy will describe performance indicators and targets to ensure common understanding among participants. Provisions for collecting information, using, and reporting the performance information will be coordinated with affected Components and the DoD CIO Council. Goal and strategy performance information will be reviewed periodically with the CIO Council and be used when preparing the annual report and updating the ITM Strategic Plan.

General Performance Approach

ITMRA directs broad implementation of the concepts of performance management. The general approach to performance is included in Appendix B, "Guiding Principles". In particular, stakeholders and outcomes have been identified in Section IV for goals and strategies. Widely accepted methods for establishing quantifiable outcome performance indicators in complex environments is discussed in the following section. Strategies and near-term actions in this plan will build a performance management environment.

Those principles are augmented by OMB and GAO guidelines and DoD guides. The *Guide for Managing Information Technology (IT) as an Investment and Measuring Performance* provides background material and a specific performance measurement development process. The *Information Management Performance Measures* produced by the National Academy of Public Administration describes an approach for developing performance measures for reporting to Congress. Additional guides are available on the WWW.

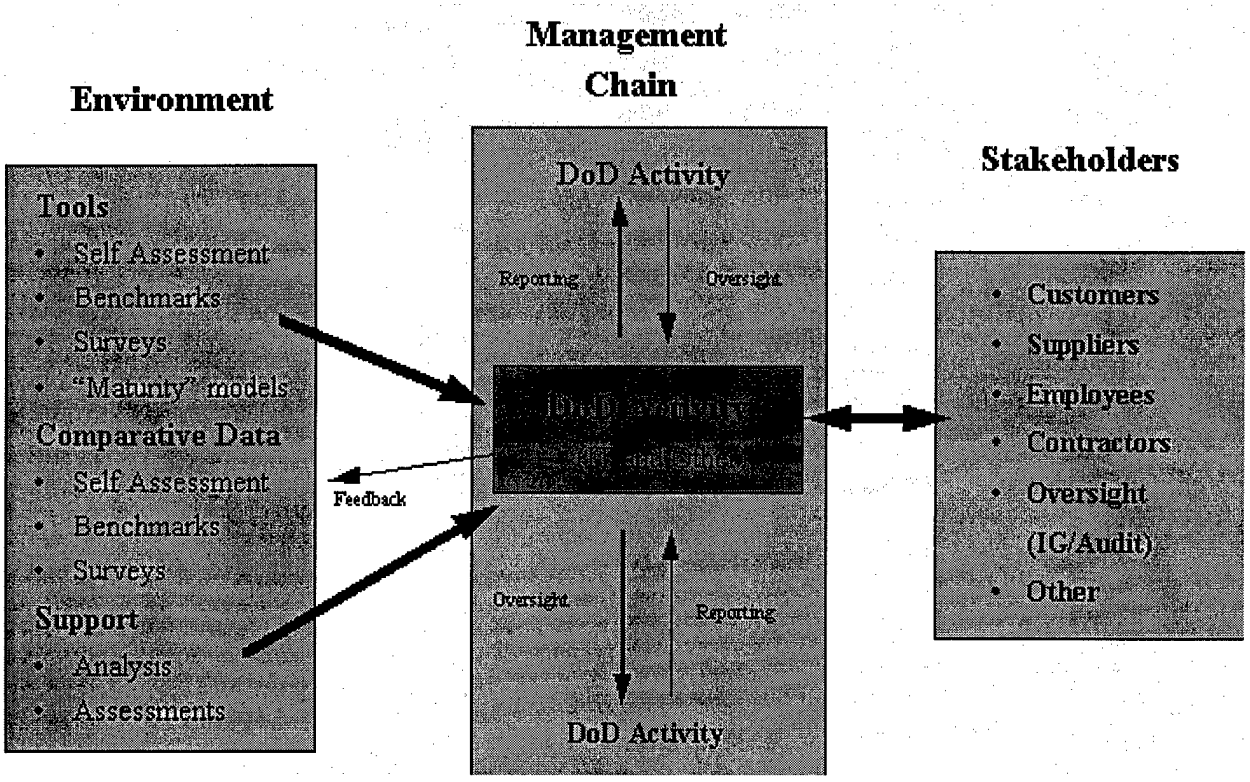
Outcome Performance Indicators for Complex Environments

Tom Peters in his book "Thriving on Chaos" said ' "What gets measured gets done" has never been so powerful a truth. Outcome measures developed with and used by management and stakeholders can be used by both parties to achieve continued satisfaction. However, these relationships are often complicated by multiple influencing factors, many subjective. Many outcome measures are not readily quantifiable. Decision support tools and methods are available to provide insight to both stakeholders and management and results can be quantified to track progress.

Performance measures at the local organizational level are the most effective. Local performance agreements between customer and supplier, adjoining management layers, or the organization to other stakeholders are the most powerful. Three types of measure methods introduced below are focused at the individual activity but the principles apply to any level organization including operating units, supply, contracting, oversight, headquarters, and information technology. In each case the activity must identify stakeholders and negotiate performance indicators that point to the quality, timeliness, etc., of the products and services.

Introducing performance management is a major activity decision. Activities often focus on the up front cost of developing strategic plans, describing performance measures, and associated contractor support. Often overlooked are the fundamental changes an activity experiences capturing and using the information, training customer and in-house personnel, and making adjustments. Establishing compelling, long-term benefits and full transition cost to the activity is critical to success.

The environment illustrated in figure D-1 can reduce the time and cost to introduce performance management and increase the quality and effectiveness. The environment provides the tools, comparative data, and access to support to effectively develop and maintain a performance management system. Consistent with empowerment, oversight and reporting are implemented within the chain of command. This creates a "learning organization". Central support needed to field quality products and assist field performance measurement are included in near-term action plans (Appendix E).



Activity Based Performance Management Environment
Figure D-1

The following outcome performance measurement approaches can be used successfully to influence positive stakeholder response and as a basis for quantitative indicators for management at all levels.

Self Assessment - The Baldrige criteria (Presidential Quality Award criteria for government) and the Software Maturity Model are well known and proven methodologies for organizational improvement. The Baldrige Award model uses a 1000 point scale divided among 7 major categories. Evaluators assist organizations to assess their effectiveness, compare with other's experience, and formulate improvement plans. The software maturity model describes a 5 level criteria for organizations to improve software development quality and efficiency. It also provides expert evaluators to help organizations determine their current status, problems, and improvement plans. Both are widely used in government and industry. Self assessment promotes policy conformance; conveying regulations as questions and suggesting actions to address problem and risk areas.

The organization performing a self assessment identifies problems and has the chance to solve them rather than adversarial inspections and oversight. Baldrige scores and maturity model levels can be used as potential quantifiable measures.

The infrastructure is in place to perform Baldrige and Software Maturity training, assessments, and also remedial training and assistance. Maturity models are available for some IT areas but more would have to be developed. Note that self assessment instruments would be the means to promulgate many ITMRA provisions; e.g., BPR before IT investments.

Benchmarks - Benchmarks are used in three contexts: (1) providing examples of new processes, ways of performing tasks, (2) determining methods of measuring and using performance, (3) comparing self to performance of others. Best business practices and quality award winners are often used as benchmarks. Some businesses have entered into partnership with others, comparing processes and performance over a number of years.

Benchmarking offers the participating organization the opportunity to learn from others in a formal way.

Comparing your cost and performance with government and commercial equivalents helps to identify and solve problems early. Externally provided benchmarks are less effective.

Extensive benchmarking databases are available. Partnering opportunities are more difficult to arrange and require commitment and openness.

Stakeholder (Customer) Surveys - Surveys can provide a reliable method to determine how others perceive an organization, its services and procedures. Standard survey tools are now emerging, like the DoD Comptroller Performance Assessment, that provide a quick, automated methods for a local activity to compose a scientific survey instrument and get customer feedback. Custom surveys provide targeted questions but require more lead time and resources.

Standard surveys are available on the WWW for a variety of situations. Using an available survey allows comparison of local results with other equivalents. Relatively simple survey instruments may be modified and used in other situations without losing reliability. Repeating a survey is critical to understanding results.

Note: OMB requires approval for surveys requiring public response "from more than 10 people". There is no legal restriction on surveying internal users.

Sample Performance Measures

Samples outlined illustrate use of the guidelines and indicators for outcome and strategy performance measures.

Sample Outcome Performance Measure - Goal 3, performance indicator (2)

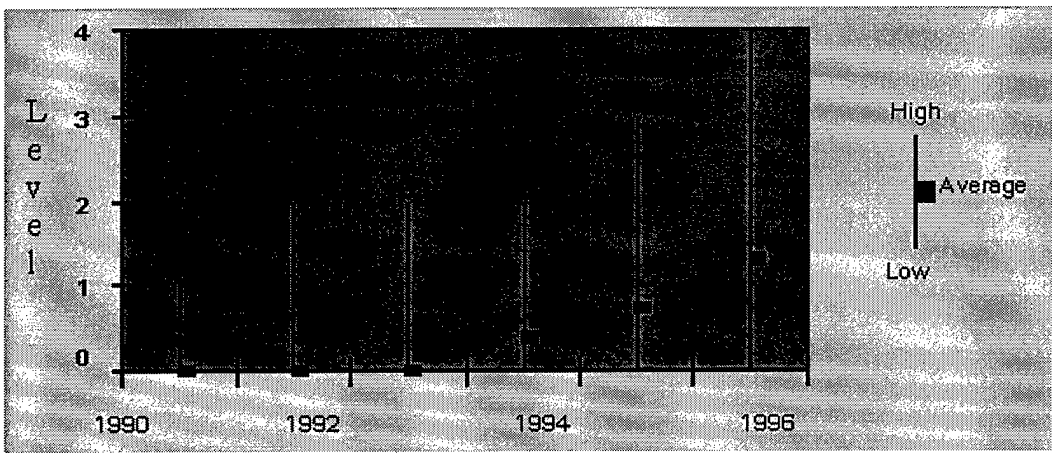
> (2) Organizational improvements can be assessed by the Presidential performance and results methodology (Baldrige criteria) supplemented by maturity models.

Sample target statement: Software development organizations achieve SEI capability maturity model level 3 by the year 2000.

Using performance guideline #8, to make the business case for the measure:

1. What is the measure supposed to show? The ability of a software organization to reliably produce quality software support.
2. Who measures and how? The organization uses the software engineering capability maturity model and trained assessors to establish the current level and actions needed to progress to the next.
3. Who uses and for what? The next level of management uses the level and action plan to evaluate organizational performance and resource requirements. DoD-wide management uses the level information as a general indication of change in software development capability.
4. How could the measure be used to subvert or be misinterpreted (unintended consequences)? Inflated evaluations could lead management to depend on an organization in critical circumstances, compromising the national defense.
5. How much will it cost to measure and what is the estimated value to the user? Using the SEI tools and techniques the cost for the initial assessment is (TDB). It allows the using activity to objectively compare it's capability with others and define a concrete action plan. Action plan includes both the cost of changes and return on investment.
6. Are there any provisions such as tools and assistance that could help? SEI provides direct assistance augmented by trained assessors.
7. Are there any critical factors that need to be considered? Use of trained assessors minimizes the opportunity for erroneous evaluations.

A typical annual report for this factor could be illustrated by Figure D-2:



Sample Graph: DoD-wide Software Capability Maturity Level by Year
Figure D-2

This chart would show that the average maturity level is increasing slowly with some activities still at level zero but a few already at level 4.

Sample Strategy Performance Measure - Strategy 2.2.2 - *Continue migration system implementation*

".. achieve acceptable levels of JTA/COE compliance by 2002 or earlier"

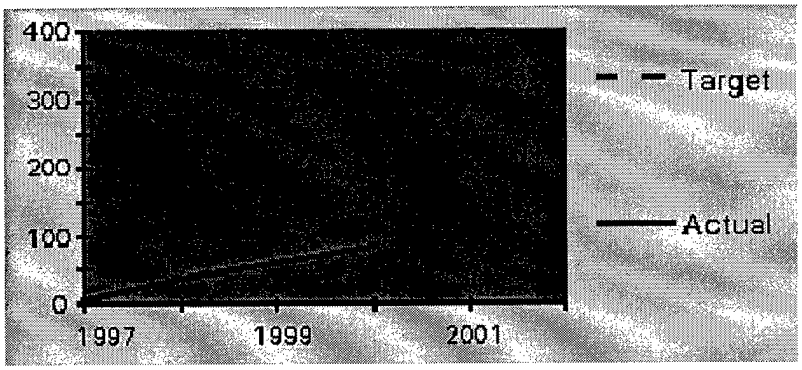
Sample target statement: Migration systems implementing COE, level 7 (out of 400 total)

- 1997 - 20
- 1999 - 175
- 2001 - 400

Using performance guideline #8, to make the business case for the measure:

1. What is the measure supposed to show? Minimum capability of migration systems to interoperate with other migration systems and make maximum use of DII capabilities.
2. Who measures and how? DISA and migration system managers run standard tests with the results recorded in the DIST.
3. Who uses and for what? DISA and migration system managers use the information for future DII planning and migration system fielding. Headquarters uses DIST summary information to determine compliance with JTA/COE and overall status of migration system developments.
4. How could the measure be used to subvert or be misinterpreted (unintended consequences)? Migration system changes after testing could compromise compliance or only system subsets are tested.
5. How much will it cost to measure and what is the estimated value to the user? Cost depends on migration systems design and implementation procedures. Cost can be minimized by employing standard interfaces and including them in routine testing. Cost to the user has not been quantified.
6. Are there any provisions such as tools and assistance that could help? Use of GCSS environment and DIST ensure consistent implementations among migration systems and installations.
7. Are there any critical factors that need to be considered? Availability and currency of test facilities to migration system developers.

A typical annual report for this factor could be illustrated by Figure D-3:



Sample Chart: Number of Migration Systems Complying with JTA/COE
Figure D-3

This chart would show actual number of migration systems complying with JTA/COE falling behind targets inviting further analysis. Reason could including reporting errors, unavailability of testing facilities, or unattainable target. The chart suggests corrective action is needed.

Summary

These examples illustrate the process to be used to discover useful performance measures in support of this strategic plan. Infrastructure to support and maintain self assessment, customer surveys and benchmarks needs to be a high priority, especially examples in Joint, DoD, and other government agency environments. Baldrige criteria and benchmarks are maintained by NIST and the TQM community. Baldrige management strategies and customer survey at IT service providers can provide a useful foundation for future application.

Appendix E - Near-Term Actions

This Appendix identifies near-term actions necessary to pursue objectives and strategies to accomplish Section IV goals. Four action categories have been identified based on the Section IV strategies:

(a) *CIO Strategic Planning Actions* - Includes activities to create and update strategic plans, performance, and supporting actions.

(b) *Develop* P*olicy, Procedure, and Methods* - Tasks to complete policy etc.

(c) *Move Out* - Energize current initiatives and launch pilots, prototypes, and plans to jump-start new strategies

(d) *Explore* - Introduce strategic analyses, tests, and experiments to address longer term issues, problem areas, and opportunities.

Each action is related to one or more strategies (*Strat*) in Section IV and an office of primary responsibility (*OPR*). The OPR oversees implementation and reports status to the CIO Council. This action list will be updated annually.

CIO Strategic Planning Actions			
Strat	*Action*	*OPR*	*Target*
Appen-dix D	Develop **performance measures** for each goal and strategy and define the annual report development process.	DoD CIO	June 1997
Appen-dix E	Refine **near-term action** plans, ensuring feasibility and resource support	DoD CIO	June 1997
3.1.1 1.3.2	Develop DoD Component **ITM Strategic Plans** including IT investment criteria and portfolio processes.	Comp CIOs	July 1997
3.1.1	Review of ITM Strategic Plan Strategy and Performance Status (Repeated annually)	DoD CIO with Comp CIO reps	August
3.1.1	Annual Strategic Planning Conference	DoD CIO	September
3.1.1	Update DoD ITM Strategic Plan (Repeated annually)	DoD CIO	October
3.1.1	Submit Annual Report	DoD CIO	October
3.1.1	Incorporate DoD ITM Strategic guidance in Component plans	Comp CIOs	

	Develop Policies, Procedures, and Methods	
Strat	*Action*	*OPR*
1.1.1	Identify a joint DoD **mission area assessment** methodology, integrate with MOP-77, and establish baseline of existing assessments.	DoD CIO
2.2.2 2.2.4	Establish methodology for **JTA/COE compliance** and test with selected migration systems and installations.	DoD CIO
2.4.2	**Combine electronic directories and access administration** into a policy, framework, and tools to include "paperless" office and information security.	DoD CIO
3.1.3	Establish **outsourcing/privatization** criteria and address related management issues including streamlined methods to define requirements and develop business cases.	DoD CIO
3.2.2	Using the maturity model process developed for software, identify other **IT management areas** for Maturity Models development and DoD-wide performance standards. and benchmarks definition	DoD CIO
3.3	Implement the CIO "certificate" **training** program	DoD CIO

	Move Out	
Strat	*Action*	*OPR*
3.1.4	Provide a DoD-wide **IT "WWW marketplace"** for any DoD user to order IT products and services	DASD (C3IA)
1.3.1	Identify DoD **processes** (including IT) for expedited **improvement** action based on potential ROI or mission performance impact.	DoD CIO/ Comp CIOs/ PSAs
2.2.1	Reengineer and **modernize mission-critical installations (bases)** in accordance with the DoD and DoD Component ITM Strategic Plans.	Comp CIOs/ JS
2.2.1	Extend **base-level metrics template** to include IT requirements and assess additional installations.	DoD CIO/ Comp CIOs
2.2.3	Establish pilot **shared data repository/warehouse** for commonly used, core mission elements with associated policy and procedures for multiple functions.	DoD CIO/ DISA/ PSAs
2.2.5	Develop **Year 2000** plans and tools to find and correct information system problems.	DoD CIO/ Comp CIOs
2.4.1	Develop high level DoD **IT simulation model** of technical, managerial, services/performance, operational aspects using the DII Master Plan as a base.	DoD CIO/ DISA
2.4.3	Establish an IT **Total Asset Visibility** repository and procedures to include user (warfighter and mission support) information service/performance requirements,	DoD CIO/ DISA
2.1.2	Extend the **DII Master Plan to include products, services & performance** for each system/program level, add C4ISR and warfighter components and compliance with JTA/COE.	DoD CIO/ DISA
3.1.4	**Streamline acquisition and oversight processes** using "Insight" concepts and procedures to increase quality and minimize disruption.	DASD (C3IA)
3.2.1	Develop a plan to **reengineer DoD IT processes** including operations, planning and approval processes and identify existing DoD IT process and data models.	DoD CIO